Notas sobre el hackeo a la Sedena (México)

5 de octubre de 2022
Jesús Pérez Caballero
El Colegio de la Frontera Norte

La comprensión del reciente robo de datos a la Sedena mexicana por un grupo de hacktivistas transnacionales (aunque todo apunta a su origen iberoamericano) requiere contextualizar algunos puntos que permitan una reflexión de mayor calado, tanto sobre este actor (seguramente, múltiple), como sobre las consecuencias para la institucionalidad oficial mexicana. Voy a estructurar mi argumentación a partir de quién realizó el ataque, qué ha supuesto y el contexto de ello:

1. *Quién.* La revelación ilegal de documentos de la Sedena la ha realizado un grupo llamado «Guacamayas». Se trata, como ya se ha dicho, de hacktivistas, es decir, de *hackers* o reveladores de información no abierta (en algunos casos, también secreta, aunque no siempre confluyen ambas categorías) con motivación ideológica. En el argot, estos hackers dizque benignos, se conocen como *white hats*, y se diferencian de otros hackers (*black hats*, *grey hats*, según su adscripción más o menos clara) que utilizan el robo de datos para comercializarlos, extorsionar y demás acciones con ánimo de lucro. Es evidente que la separación no es clara. No lo es porque, al realizar un robo de datos es posible que, a su vez, estos sean distribuidos con facilidad; así, bastaría identificarse como periodista y explicar por qué se quieren los documentos para obtener el archivo hackeado por Guacamayas a través de las webs Enlace Hacktivist y Distributed Denial of Secrets. Esa es una barrera mínima y permite que particulares con ánimo de lucro, organizaciones criminales o servicios de inteligencia extranjeros se hagan con los documentos.

Aun así, el énfasis ideológico de «Guacamayas» es claro; podemos entenderlo doblemente. Por un lado, es nítido su anarquismo primitivista, de ahí el nombre, del taíno «guacamayo», referente a esta ave. Fuentes colombianas señalan que serían centroamericanos, si bien, por la naturaleza de estas acciones de hacktivismo, es fácil concitar a individuos de distintas nacionalidades, eso sí, podría haber indicios de ello por su presentación mediática para atacar al ministerio guatemalteco de minas, tal y como señalaron los hacktivistas en una entrevista en la web de investigación periodística *Forbidden Stories*. Aun así, cabe recordar que su primer ataque fue contra una unidad del ejército de Chile.

En cualquier caso, su ideología está claramente basada en John Zerzan y sus epígonos (estoy pensando en el brumoso grupo Individualistas Tendiendo a lo Salvaje, en México, aunque en Guacamayas no existe ninguna apelación a la violencia, lo que los separa claramente del ecoterrosimo), esto es individuos que hipostasian, hasta la sublimación, a la naturaleza («No somos defensoras de la naturaleza, somos la naturaleza», señalan al principio y al final de un comunicado, tan cursi como su poema de presentación). Así, pretenden volver a situaciones sin Estado, ni industria (que, para ellos, como neoludistas rousseaunianos, se reducen, *emic*, a psicologistas «ansias de dominio»), de cazadores recolectores o formas de autosubsistencia e interacción interespecie idealizadas. Como novedad de «Guacamayas», estaría a) el giro indigenista («Nuestra Pachamama, madre de la que venimos»; «Servirá para honrar a nuestra Pachamama y nuestras ancestras», se lee en su comunicado, repleto de alusiones al mito del *Abya Yala*, esto es, un ecumenismo de cosmovisiones indígenas americanas); y b) la retórica contra el desarrollo industrial canalizado en el rechazo a las mineras (extractivismo, neoextractivismo, extractivismo global y demás combinaciones académicas).

Por otro lado, estratégicamente, el grupo está en la tradición de filtraciones de Anonymous, WikiLeaks o Phineas Fisher, con el denominador común de apelar a un movimiento antiseguridad (*antisec*), es decir, a la crítica a un complejo industrial securitario donde instituciones políticas, empresas y agencias de seguridad civiles o militares serían lo mismo. De nuevo, el denominador común, es el anarquismo: cualquier Estado (quizá, cualquier industria como «fuerzas represivas»), según sus parámetros maximalistas, ya es culpable por existir, y también lo sería cualquier acción que no retrotraiga la historia a antes de 1492. Es evidente que ante ese sectarismo de brocha gorda, sin matices — meten en el mismo saco a Obrador y a Boric, a Bolsonaro y Bukele; a empresas mineras de capital chino y a los ministerios mineros de Colombia o Guatemala; a la Policía Nacional de El Salvador y a la Sedena mexicana — solamente pueden actuar del modo que actúan, porque, dado el delirio ideológico, serían incapaces de competir en términos de partidos o ni siquiera intervenir en una plática entre la población de los países cuyas instituciones atacan. Este delirio, como nos muestra la historia, no significa que no tengan una racionalidad suficiente para mostrar destrezas tecnológicas y solidez estratégica para marcar objetivos, que les permita sostener una agenda bastante clara de posicionamiento de su mensaje

cuando se leen sus declaraciones. Y si bien estos hacktivistas aluden a cuestiones que quienes vivimos en México sabemos, como la confluencia de intereses entre instituciones públicas y privadas, incluso criminales, o la capacidad de influencia, a veces también delincuencial, de multinacionales mineras, más bien las parasitan para dar salida a su discurso idealista neoprimitivista.

2. *Qué*. El ataque que se ha realizado a la Sedena se caracteriza por los siguientes rubros:

— *Cuantitativo*. Sigo a Manuel Rivera cuando señala que el ataque «[e]quivale a 39 millones de páginas de Word o PDF; o 1.5 millones de fotos, o 3,000 horas de video». Este experto lo compara a otros robos: el ataque a la Sedena es «2.3 veces la filtración de información de Panama Papers (2.6 TB); poco más del doble de la de los Pandora Papers (2.9 TB)».

— *Indiscriminatorios*. A diferencia de los objetivos de elites o fortunas que tenía la investigación de los Panama o Pandora Papers, en este caso, la información es masiva, pero sin que haya una labor previa de curaduría o selección. Esto, paradójicamente, minimiza el impacto: se requieren aptitudes de investigación e incluso gestión de *Big Data* y manejo de documentos para comprenderlos en su cabalidad, por lo que quienes tienen los documentos relevados (el diario español *El País*, ha reconocido tener ya «más de cuatro millones de documentos con conversaciones, órdenes, partes, estados de cuentas y notas informativas entre mandos altos y medios desde el año 2010 hasta septiembre 2022»; la web mexicana de análisis de documentos desclasificados *Archivero* afirma estar estudiándolos, etcétera) deben hacer una labor de criba de qué es importante y qué no. ¿Qué significa esto? Que es probable que estos documentos aparezcan en corto, medio o largo plazo en el debate público, y sean susceptibles de ser utilizados en investigaciones, pero también en campañas, sea electorales o de otro tipo, como ya se hizo con los de WikiLeaks (por ejemplo, contra la ex candidata demócrata estadounidense Hillary Clinton).

Eso sí, es necesario diferenciar «secreto» de «no público». Muchos documentos (que se pueden consultar sin hacer una petición expresa que sí aplica para archivos más pesados) hablan de un monitoreo propio de las labores de inteligencia que se presuponen a la institución, por ejemplo, en sus rutinarios «Diarios de Información y Análisis» (ejemplo); puede criticarse ese afán de control del ejército mexicano, pero eso no es ilegal y muchos

de esos documentos, efectivamente, pueden consultarse por transparencia (otra cosa es lo capcioso de algunos presupuestos sobre esa transparencia).

Cuestión distinta es qué hay de lo revelado que sea secreto, lo que podría suponer crisis de Estado que la institucionalidad oficial mexicana debería anticipar. Así, es evidente lo urgente de un grupo de expertos en la administración obradorista que analice qué se ha filtrado y separe lo que era susceptible de publicarse, lo que sin ser secreto puede exponer a la Sedena y lo que sea secreto, sea por derecho a la intimidad o por aludir al secretismo a los que algunos temas obligan (los *arcana imperii*).

Con todo esto, me refiero a una cuestión material, objetiva, de qué es secreto, y no a lo que se señale formalmente como secreto o reservado, de una manera extralimitada. Por ejemplo, si hay implicadas violaciones graves de derechos humanos esa reserva debería ser ilegal. Tampoco deberían reservarse contratos que se dan a la Sedena para que haga obra pública o las circunstancias del robo de información por «Guacamayas» (es habitual en México reservar la información sobre graves ataques informáticos a instituciones públicas).

3. *Contexto*. Debemos entender que el foco de ataques de «Guacamaya» ha virado, y lo hecho, seguramente, sondeando qué prende mediáticamente y qué no. Así, su selección de blancos (*targeting*) ha sido:

a) En primer lugar, se produjo (en mayo de 2022) un ataque al Estado Mayor Conjunto (EMCO), organismo asesor del Ministerio de Defensa en materia de Fuerzas Armadas de Chile (400,000 correos electrónicos divulgados). En este caso, los hackers señalan en entrevista reciente que el Estado chileno ya había sido advertido por expertos de ese posible fallo.

b) Posteriormente, se realizó un mayor despliegue para exponer a empresas mineras polémicas o, incluso, que pudieran haber cometido hechos delictivos, o a la institución pública que concede las licitaciones. Así, en Extractivists Leaks, con fecha del 3 de agosto de 2022 , se reveló información de:

Institución	**País**	**Grupos afectados**	**Fuente**
Quiborax	Chile	Quechua	https://archive.vn/3R3WL
Empresa nacional Minera (ENAMI EP)	Ecuador	Mestizos y afroecuatorianos	https://archive.vn/AFxDl
Agencia Nacional de Hidrocarburos	Colombia	Población en general (empresa encargada de licencias y reparto de regalías)	https://www.anh.gov.co/es/
New Granada Energy	Colombia y China	Población de Paz de	https://archive.ph/IY4fN

Corporation (filial de la estatal china Sinopec)		Ariporo (Departamento de Casanare)	
Oryx Resources	Venezuela	Población	https://archive.ph/wip/MPdK7
Tejucana Mineração	Brasil	Población de Brumandinho (estado de Minas Gerais, Región Metropolitana de Belo Horizonte)	https://archive.ph/wip/l7sRY
Ministerio de Ambiente y Recursos Naturales	Guatemala	Población en general (empresa encargada de licencias y reparto de regalías)	https://archive.ph/m0WZk https://archive.ph/wip/lFyUh

c) Finalmente — al menos, hasta la fecha —, se volvió a atacar a entidades del ámbito securitario, pero de un modo coordinado y transnacional. Además de la Sedena de México (6 TB), se ha revelado información en septiembre de 2022:

1. Policía Nacional Civil de El Salvador (4 TB)
2. Comando General de las Fuerzas Militares de Colombia (275 GB)
3. Fuerza Armada de El Salvador (50 GB)
4. Comando Conjunto de las Fuerzas Armadas de Perú (35 GB)
5. Ejército de Perú (70 GB)

Sin embargo, solo en el ataque a la Sedena mexicana se ha logrado un impacto mediático a nivel de país, seguramente por la condición de México (país mayor que los anteriores, cercanía con EEUU), así como por aspectos como las polémicas por el espionaje de Pegasus, el debate sobre la militarización de la seguridad pública (y, en general, la susceptibilidad del uso de estas informaciones en un contexto de polarización política), y el mismo rol del ejército mexicano en temas de diferente índole. Tal vez por eso, la filtración a la Sedena ha contado con la simpatía mediática y, en parte, poblacional: por haberse realizado contra una institución percibida como la que está acumulando más poder en el gobierno federal (tampoco puede descartarse la coyuntura sobre el caso Ayotzinapa y el rol discutido de esta institución en esas icónicas desapariciones).

Referencias

Bueno, Gustavo, «La nostalgia de la barbarie, como antiglobalización», Antílogo al libro de John Zerzan, *Malestar en el tiempo*, Ikusager, Vitoria, 2001, https://www.filosofia.org/aut/gbm/2001zer.htm

Comunicado de «Guacamayas», https://enlacehacktivista.org/comunicado_guacamaya2.txt

Colleman, Gabriella, *Hacker, Hoaxer, Whisteblower, Spy. The Many Faces of Anonymous*, Londres-Nueva York, Verso, 2014.

Enlace Hacktivista, *Extractivist Leaks*, https://enlacehacktivista.org/index.php?title=Extractivist_Leaks/es (wiki creada el 1 de agosto de 2022)

Enlace Hacktivista, *Fuerzar Represivas*, https://enlacehacktivista.org/index.php?title=Fuerzas_Represivas (wiki creada el 19 de septiembre de 2022)

Mennickent Barrios, Camila, «Hablan hackers: revelan que Estado Mayor Conjunto "eligió" no reparar falla que posibilitó ataque», *Biobiochile*, 28 de septiembre de 2022, https://www.biobiochile.cl/especial/bbcl-investiga/noticias/reportajes/2022/09/28/hablan-hackers-revelan-que-estado-mayor-conjunto-eligio-no-reparar-falla-que-posibilito-ataque.shtml

Muñoz, Gabriela, «Reflexión sobre el Ecoterrorismo», *Colef Press*, 10 de octubre de 2019, https://www.youtube.com/watch?v=TQgzrJD-H4U

Richard, Laurent, «La lucha por un territorio es la lucha de todas» », *Forbidden Stories*, 6 de marzo de 2022, https://archive.ph/I9E4n (entrevista a «Guacamayas»)

Rivera, Manuel, «Qué es un hacktivista y otras preguntas que surgen tras el ciberataque a Sedena», *Business Insider México*, 4 de octubre de 2022, https://businessinsider.mx/hacktivista-dudas-hackeo-sedena-guacamara-infosecurity-mexico_tecnologia/